FRENCH REPUBLIC

Ministry of Health and Access to Health Care

Order of XX amending the Order of 20 November 2023 amending the Order of 23 October 2023 amending the Order of 23 June 2022 on the criteria applicable to the referencing of digital services and tools to the Digital Health Space Service Catalogue

NOR: SPRD2310767A

The Minister for Health and Access to Health Care,

Having regard to Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down an information procedure in the field of technical regulations and of rules on Information Society services, and in particular Notification No. 2022/083/F;

Having regard to the Public Health Code, in particular Articles L. 1470-5, R. 1111-37 and R. 1111-39 thereof;

Having regard to the Order of 23 June 2022 on the criteria for referencing digital services and tools in the digital health space service catalogue;

Having regard to the Order of 23 October 2023 on the criteria for referencing digital services and tools in the digital health space service catalogue;

Having regard to the Order of 20 November 2023 on the criteria for referencing digital services and tools in the digital health space service catalogue;

Order:

Article 2

The annex to the above-mentioned Order of 20 November 2023, entitled ‘Reference framework V2 for the benchmarks for a digital tool or service in “My Health Area”’, is replaced by the document annexed to this Order, entitled ‘Reference framework V3 for the benchmarks for a digital tool or service in “My Health Area”’.

Article 3

The Delegate for Digital Health is responsible for the execution of this Order, which shall be published in the *Official Journal* of the French Republic.

Done on XX 2025,

For and on behalf of the Minister:

The Delegate for Digital Health

H. Ghariani

ANNEX – Reference framework V3 for the benchmarks for a digital tool or service in 'My Health Area'

The criteria are divided into seven thematic lists of questions according to the nature of the candidate applications for referencing: two specific lists of questions for applications that already have a certificate of conformity from the Digital Health Agency, four generic lists of questions ('urbanisation', 'interoperability', 'security maturity' and 'ethics') and one additional list of questions specific to referencing with data exchange ('security for referencing with data exchange'). The lists of questions should be completed on the Convergence platform made available by the Digital Health Agency.

For generic lists of questions 'urbanisation', 'interoperability', 'security maturity', the criteria for which the answers are graduated may consist of between two and four levels numbered from 0 to 3. The list of criteria detailed below contains only the levels defined and accessible on the 'Convergence' platform.

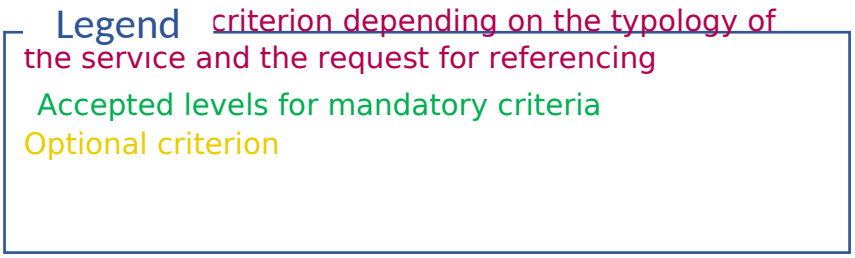
For the list of questions on 'ethics', the answers given for the criteria are: 'Non-conformant' or 'conformant' If it is indicated that the mandatory 'ethics' criterion is compliant, one or more supporting documents must be provided to justify the fulfilment of the criterion.

For the list of questions 'security for referencing involving data exchange', the publisher must, on the 'Convergence' platform, download a dedicated form, and after completing it, submit it along with the associated exculpatory evidence.

In addition, in order to justify the fulfilment of certain optional criteria, supporting documents must be produced and kept available by the publisher with a view to the ongoing evaluation of the digital service; they are not to be provided at the time of the initial application.

Whether or not the answers to the lists of questions are required or not depends on the type of digital tool or service and the type of referencing desired (with/without data exchange with 'My Health Area'). This conditioning is carried out on the 'Convergence' platform by means of an orientation list of questions describing the digital tool or service and the owner's request. Obtaining a certificate of conformity with the sectoral repositories adopted by the NSA (digital medical devices or tele-consultation company) makes it possible to fulfil the conditions laid down in Article R1111-37 of the Public Health Code to allow the referencing of a tool to the service catalogue.

Contents



1. Digital medical device journey

DMN 1.1 – Possession of a valid DMN certificate

The manufacturer MUST have a final certificate of conformity with the valid Digital Medical Devices Interoperability and Safety Framework (DMN), provided for in Article L. 1470-5 of the Public Health Code drawn up by the Public Interest Grouping mentioned in Article L. 1111-24 of the Public Health Code (NSA) and the candidate application for referencing MUST be included in the scope of the certificate of conformity.

a. Supporting documents: the final certificate of conformity with the DMN Interoperability and Security Framework

2. Journey dedicated to tele-consultation corporations

TLC 1.1 – Possession of a valid TLC certificate

The manufacturer MUST have a final certificate of conformity with the valid Interoperability, Security and Ethics Framework for Remote Consultation SI, provided for in Article L. 1470-5 of the Public Health Code established by the Public Interest Grouping mentioned in Article L. 1111-24 of the Public Health Code (NSA) and the candidate application for referencing MUST be included in the scope of the certificate of conformity.

a. Supporting documents: the final certificate of conformity with the interoperability, security and ethics framework of remote consultation SIs

3. Generic listing journey

a. Urbanisation

A06. Electronic identification of patients, users or persons

A06.1 Implementation of the INS (for services where user data is accessible by healthcare professionals)

- Level not applicable: Always applicable if the criterion appears.
- Level 0: The product is not authorised by the CNDA to use the INSi teleservice and has not incorporated the features of the INS.
- Level 1: The product is authorised by the CNDA to use the INSi teleservice.
- ✓Level 2: The product is authorised by the CNDA to use the teleservice INSi and has incorporated all the requirements applicable to the product of the INS Implementation Guide.

A06.2 Integration of identity traits (for services that contribute towards prevention or care without user data being directly accessible to healthcare professionals)

- Level not applicable: Always applicable if the criterion appears.
- Level 0: The product has not integrated the completeness of the following identity traits: name at birth, first name, date of birth, wording of the city of birth, department of birth, sex, surname used (if different from name at birth), first name used (if different from first name at birth).
- ✓Level 1: In the creation and management of user identities, the product has incorporated the following traits: name at birth, first name, date of birth, wording of the city of birth, department of birth, sex, surname used (if different from name at birth), first name used (if different from first name).
- ✓Level 2: Conformant with the previous level, plus: the wording of the city of birth is collected with the Official Geographical Code of the INSEE in consistency with the date of birth.

b. Interoperability

A08.1 Interoperability reference framework (background information)

A08.1.1 Use and enhancement of the CI-SIS

- Level not applicable: Always applicable if the criterion appears.
- Level 0: No interoperability principle is integrated into the product design.
- Level 1: The product was designed without systematic reference to the interoperability standards proposed by the CI-SIS.
- Level 2: The product was designed with systematic reference to the interoperability standards proposed by the CI-SIS. Uses not covered by the CI-SIS are not brought to the attention of the NSA [National Safety Authority] and are implemented by proprietary developments.
- Level 3: The product was designed with systematic reference to the interoperability standards proposed by the CI-SIS. Any uses not covered are systematically brought to the attention of the NSA, so that the Interoperability Framework for Healthcare Information Systems can be continuously improved. These uses are implemented through developments based on the interoperability standards on which the CI-SIS is based.

A08.3 Interoperability reference framework (transmission)

A08.3.1 Synchronous connection with other SIs

- Level not applicable: Always applicable if the criterion appears.

- Level 0: The connection with other SIs is done via standards other than those identified in the CI-SIS (e.g. VPN and MLLP for WAN, FTP, CFT connections, ...).
- Level 1: The connection with other SIs is done via the standards identified in the CI-SIS without exactly meeting all the specifications of one of the criteria of the transmission layer of the CI-SIS (synchronous transport for thick clients or synchronous transmission for mobile or web applications).
- Level 2: The connection with other SIs is done according to the specifications of one of the criteria of the transmission layer of the CI-SIS (synchronous transport for thick clients or synchronous transmission for mobile or web applications).
- Level 3: The connection with other SIs is done according to the specifications of one of the criteria of the transmission layer of the CI-SIS (synchronous transport for thick clients or synchronous transmission for mobile or web applications) and the elements provided in the HIVF contribute to the implementation of the security policy (right of access, traceability, etc.).

A08.4 Interoperability reference framework (service)

ℹ A08.4.1 Interoperable implementation of the Health Document Sharing service

- Level not applicable: Always applicable if the criterion appears.
- Level 0: The uses of the product corresponding to the Health Document Sharing service are implemented in a proprietary manner without reference to the CI-SIS specifications.
- Level 1: The uses of the product corresponding to the Health Document Sharing service are implemented using the standard guidelines of the CI-SIS without strictly following them.
- Level 2: The uses of the product corresponding to the Health Document Sharing service are implemented with some major changes (e.g. specific extensions, proprietary names, etc.) which are the subject of CI-SIS development requests.
- Level 3: The uses of the product corresponding to the Health Document Sharing service are implemented without any major changes (i.e. without the extension of specifications).

ℹ A08.4.6 Interoperable implementation of the Shared Schedule Management service

- Level not applicable: Always applicable if it appears.
- Level 0: The uses of the product corresponding to the Shared Schedule Management component are implemented in a proprietary manner without reference to the CI-SIS specifications.
- Level 1: The uses of the product corresponding to the Shared Schedule Management component are implemented using the standard guidelines of the CI-SIS without strictly following them.
- Level 2: The uses of the product corresponding to the Shared Schedule Management component are implemented with some major changes (e.g. specific extensions, proprietary names, etc.) which are the subject of CI-SIS development requests.
- Level 3: The uses of the product corresponding to the Shared Schedule Management component service are implemented without any major changes (i.e. without the extension of specifications).

ℹ A08.4.8 Interoperable implementation of the Health Measures service

- Level not applicable: Always applicable if it appears.
- Level 0: The uses of the product corresponding to the Health Measures service are implemented in a proprietary manner without reference to the CI-SIS specifications.
- Level 1: The uses of the product corresponding to the Health Measures service are implemented using the standard guidelines of the CI-SIS without strictly following them.
- Level 2: The uses of the product corresponding to the Health Measures service are implemented with some major changes (e.g. specific extensions, proprietary names, etc.) which are the subject of CI-SIS development requests.
- Level 3: The uses of the product corresponding to the Health Measures service are implemented without any major changes (i.e. without the extension of specifications).

A08.5 Interoperability reference framework (business content)

A08.5.01 Minimum structuring document for apportionment and/or document exchange (producer of SAF documents)

- Level not applicable: The product does not produce health documents.
- Level 0: The product produces health documents but cannot produce SAF documents (production restricted to PDF, Word, TxT etc. file types).
- ✓ Level 2: The product produces health documents and can produce SAF documents without fully following the minimum structuring component of health documents (regardless of the level of structuring of the body of the SAF).
- ✓ Level 3: The product produces health documents and can produce SAF documents while fully implementing the minimum structuring component of health documents (regardless of the level of structuring of the body of the SAF).

A08.5.23 Minimum structuring for apportionment and/or document exchange (consumer of SAF documents)

- Level not applicable: The product does not consume any SAF documents.
- Level 0: The product does not have SAF document display capabilities.
- Level 1: The product has unstructured body SAF document display capabilities, but cannot display the headers or bodies of SAF documents with structured bodies.
- ✓ Level 2: The product has the ability to display SAF documents (regardless of the level of structuring of their body) without interpreting their content. The product also allows manual registration by the user.
- ✓ Level 3: The product has the ability to display SAF documents (regardless of the level of structuring of their body) with interpretation of the SAF header for automatic or semi-automatic processing (e.g., recording in the patient record).

A10. Health terminology

A10.2 Use of NSA nomenclatures

- Level not applicable: Always applicable if the criterion appears.
- Level 0: Use of local nomenclatures not made available by the NSA.
- Level 1: Use of part of the nomenclatures made available by the NSA supplemented by local codes. No requests for updates were made to the NSA.
- Level 2: Use of nomenclatures made available by the NSA with definition of the JDV if appropriate.
- Level 3: Use of nomenclatures made available by the NSA with definition of the JDV if appropriate. If necessary, a request was made to update the nomenclatures made available by the NSA to take into account the needs of the company.

c. Safety maturity

01. SSI Governance

01.01 - Designation of stakeholders responsible for monitoring and maintaining security measures

- Level not applicable: Always applicable
- Level 0: Within the product team, those responsible for security and those responsible for implementing and monitoring security measures are not formally defined and appointed.
- ✓ Level 1: Within the product team, those responsible for security are identified. Their responsibilities cover design, development, installation, operation, administration and maintenance activities (depending on the scope for which the manufacturer is responsible for the user structure).
- ✓ Level 2: The same as the previous level, plus: For each of these stakeholders, a substitute is identified to replace them in case of absence, who has the necessary knowledge and rights to ensure they can fill in the role adequately.
- ✓ Level 3: The same as the previous level, plus: For each planned security measure, a responsible person is identified, who must ensure its proper implementation and effective functioning.

01.04.01 - Raising awareness among the teams in charge (for services that do not exchange data with My Health Area and/or contain personal data)

- Level not applicable: Always applicable
- Level 0: There is no raising awareness conducted among the teams in charge of design, development, installation, administration and maintenance activities (depending on the scope for which the manufacturer is responsible for the user structure).
- ✓ Level 1: There is a general raising of awareness regarding risks for all teams (on issues and risks). If the product is intended to process personal data or health data, sensitisation includes specific obligations and rules of behaviour in this regard.
- ✓ Level 2: The same as the previous level, plus: A good handling of the subject by the stakeholders is measured. Sensitisation is regularly refreshed. The participation of each stakeholder is tracked.
- ✓ Level 3: The same as the previous level, plus: Sensitisation includes a component specific to the activities of each team (specific challenges/risks/SIS procedures).

01.04.02 – sensitisation of the teams in charge

- Level not applicable: Always applicable
- Level 0: There is no raising awareness conducted among the teams in charge of design, development, installation, administration and maintenance activities (depending on the scope for which the manufacturer is responsible for the user structure).
- Level 1: There is a general raising of awareness regarding risks for all teams (on issues and risks). If the product is intended to process personal data or health data, sensitisation includes specific obligations and rules of behaviour in this regard.
- ✓ Level 2: The same as the previous level, plus: A good handling of the subject by the stakeholders is measured. Sensitisation is regularly refreshed. The participation of each stakeholder is tracked.
- ✓ Level 3: The same as the previous level, plus: Sensitisation includes a component specific to the activities of each team (specific challenges/risks/SIS procedures).

03. Safe design

03.12 – product integrity

- Level not applicable: Always applicable if the criterion appears
- Level 0: There is no mechanism to verify that installed software components and product configuration have not been altered.
- ✓ Level 1: There is a mechanism to verify that installed software components and product configuration have not been accidentally altered. These mechanisms can be specific to the product or rely on environmental features required for the product (operating system, etc.)
- ✓ Level 2: A solution is provided to verify that the installed software components of the product have not been altered accidentally or voluntarily and unauthorised (potentially more elaborate and complex alteration than accidental alteration).
- ✓ Level 3: The same as the previous level, plus: the solution used also makes it possible to verify that the configuration of the product has not been accidentally or intentionally altered and unauthorised.

03.13.01 - Information protection (Cryptography) (for services that do not exchange data with My Health Area and/or contain personal data)

- Level not applicable: Always applicable if the criterion appears
- Level 0: Some exchanges of sensitive information (password, authentication token, personal data, etc.,...) are not encrypted, are not subject to verification of their integrity or their recipient is not authenticated.
- ✓ Level 1: Sensitive information is always protected during communications on public channels (Internet) or external to the user structure: the recipient is authenticated prior to the exchange, the data is encrypted and their integrity verified.
- ✓ Level 2: Sensitive information is always protected during communications using any type of internal or external channel: the recipient is authenticated prior to the exchange, the data is encrypted and their integrity verified. As an exception, the encryption of sensitive data is not

required in cases of communication: - with peripherals in the immediate vicinity of the workstations where the product is installed; – with communicating medical devices; provided that the means of communication used are dedicated to that use and pass and extend exclusively into premises with controlled access by physical means (lockdown, digicode, etc.). Only a major reason can justify an exception to these requirements, and any exception must be clearly documented and justified in the product documentation. The documentation of the product explains these safety requirements for the implementation of the product, for the attention of user structures.

- ✓ Level 3: The same as the previous level, plus: Risk-appropriate and justified protection mechanisms shall be implemented, in particular with regard to the encryption of sensitive information that is transmitted or stored. The encryption, integrity verification, and authenticity algorithms, and more generally the cryptographic mechanisms used and the corresponding key sizes are state-of-the-art, in accordance with the rules set out by the RGS, the TLS Security Recommendations (v1.2+) and the Cryptographic Mechanisms Guide (v2.0.4+), published by the ANSSI. The mechanisms used by the product are reviewed regularly to remain conformant with these recommendations.

❗03.13.02 - Protection of personal data (Cryptography) (for services that exchange data with My Health Area)

- Level not applicable: Always applicable if the criterion appears
- Level 0: Some exchanges of sensitive information (password, authentication token, personal data, etc.,...) are not encrypted, are not subject to verification of their integrity or their recipient is not authenticated.
- Level 1: Sensitive information is always protected during communications on public channels (Internet) or external to the user structure: the recipient is authenticated prior to the exchange, the data is encrypted and their integrity verified.
- Level 2: Sensitive information is always protected during communications using any type of internal or external channel: the recipient is authenticated prior to the exchange, the data is encrypted and their integrity verified. As an exception, the encryption of sensitive data is not required in cases of communication: - with peripherals in the immediate vicinity of the workstations where the product is installed; – with communicating medical devices; provided that the means of communication used are dedicated to that use and pass and extend exclusively into premises with controlled access by physical means (lockdown, digicode, etc.). Only a major reason can justify an exception to these requirements, and any exception must be clearly documented and justified in the product documentation. The documentation of the product explains these safety requirements for the implementation of the product, for the attention of user structures.
- ✓ Level 3: The same as the previous level, plus: Risk-appropriate and justified protection mechanisms shall be implemented, in particular with regard to the encryption of sensitive information that is transmitted or stored. The encryption, integrity verification, and authenticity algorithms, and more generally the cryptographic mechanisms used and the corresponding key sizes are state-of-the-art, in accordance with the rules set out by the RGS, the TLS Security Recommendations (v1.2+) and the Cryptographic Mechanisms Guide (v2.0.4+), published by the ANSSI. The mechanisms used by the product are reviewed regularly to remain conformant with these recommendations.

❗ 03.14 - Secret management (private keys and passwords)

- Level not applicable: Always applicable if the criterion appears
- Level 0: There is no explicit secret management principle for the product.
- Level 1: Secret management principles are explicitly defined for the product. Some secrets used by the product (symmetric keys, private keys, passwords, etc.) are stored in clear text in the configuration files.
- ✓ Level 2: Secret management principles are explicitly defined for the product. The symmetrical and private keys of certificates are accessible only by a restricted and privileged account (e.g.: “root”) and are read-only outside the operations of changing these secrets. If passwords are

managed within the product, they are stored in a form that definitively prohibits access to their value in plain text.

- ✓ Level 3: The same as the previous level, plus: If accesses are provided from outside the structure hosting the product (Internet, other third parties), then: either a bastion system is set up in order to centralise these accesses by secured connections from outside and to protect the secrets used for the actual connections to the product; or the symmetric keys and private keys used for these connections are confined in a secure component that carries out all the cryptographic functions mobilising these keys and used for the actual connections to the product and from which they cannot be extracted.

❗ 03.15 - Encryption of storage media

- Level not applicable: Always applicable if the criterion appears
- Level 0: Not all data storage media inside the mobile equipment are encrypted.
- ✓ Level 1: All data storage media inside the mobile equipment are encrypted.
- ✓ Level 2: The same as the previous level, plus: Encryption keys are exclusively controlled by the user structure, either directly or via mobile equipment management software.
- ✓ Level 3: The same as the previous level, plus: Mechanisms in accordance with the RGS and the guide to cryptographic mechanisms (v2.0.4+), published by ANSSI, are implemented for this purpose. The mechanisms used by the product are reviewed regularly to remain conformant with these recommendations.

❗03.18 Documentation and good practices

- Level not applicable: Always applicable if the criterion appears
- Level 0: No documentation (one or more documents) specifies best practices and/or procedures for secure development and configuration
- ✓ Level 1: Documentation (one or more documents) setting out best practices and/or procedures for secure development and configuration MUST be available and followed for the creation of the system and the implementation of new functionalities. This documentation must address at least the following points:
    - Safe design
    - Symbol of the quality grade of the code
    - Management of the obsolescence of software components
    - Safety tests
    - Patch deployment

04. Identification, authentication and authorisations

❗ 04.01 - Use and updating of national identities of natural health stakeholders

- Level not applicable: Always applicable if the criterion appears
- Level 0: The product is unable to identify healthcare professionals using a national identity (RPPS, and ADELI which is being phased out) or a pre-existing local identity in the user structure (HR number, etc.).
- Level 1: The product does not correspond to a 'sensitive' digital service as defined in the PGSSI-S natural health stakeholders' electronic identification repository. It can identify health stakeholders using the national identity (RPPS, and ADELI which is being phased out) or a pre-existing local identity in the user structure (HR registry, etc.). These identities can be edited through a documented management process.
- Level 2: If the product corresponds to a 'sensitive' digital service as defined in the PGSSI-S electronic identification repository for natural health stakeholders, it shall comply with that same repository. In particular, it identifies health stakeholders at least using the national identity (RPPS, and ADELI which is being phased out).
- ✓ Level 3: The same as the previous level, plus: The documented management process systematises searches/verifications with the Reference repository (RPPS) and limits changes to attributes that are absent from the national identity as visible on the Health Directory and other

exposure layers of the RPPS. Checks on the exposure layers of the RPPS (import of flat files, programming interfaces, etc.) are carried out on a regular basis or in connection with transactions carried out by the users concerned (electronic identification, etc.), in compliance with regulatory requirements.

04.02 - Guarantee level of electronic identification of natural health stakeholders

- Level not applicable: Always applicable if the criterion appears
- Level 0: The product corresponds to a 'sensitive' digital service as defined in the PGSSI-S electronic identification repository for natural health stakeholders, but it does not comply with that same repository, or the product does not correspond to a 'sensitive' digital service and does not ensure the electronic identification of its users who are natural health stakeholders.
- Level 1: The product does not correspond to a 'sensitive' digital service as defined in the PGSSI-S electronic identification repository for natural health stakeholders. It ensures the electronic identification of its users that are natural health stakeholders, but it does not comply with the requirements of the same repository applicable to sensitive services (which are not enforceable against it).
- ✓ Level 2: If the product corresponds to a 'sensitive' digital service as defined in the PGSSI-S electronic identification repository for natural health stakeholders, it shall comply with the requirements of that same repository relating to the electronic identification. In particular, the product implements electronic identification via Pro Santé Connect. The product implements at least one electronic identification means within the framework of the transitional electronic identification means (with an enhanced 'eIDAS' guarantee level) as defined by the above-mentioned reference framework.
- ✓ Level 3: The same as the previous level, other than: The product does not implement any electronic identification means within the framework of the transitional electronic identification means defined in the PGSSI-S electronic identification repository for natural health stakeholders.

04.03 - Guarantee level of electronic identification of patients or users

- Level not applicable: Always applicable if the criterion appears
- Level 0: The product provides access to personal data to users or patients, but does not comply with the PGSSI-S user identification repository.
- ✓ Level 2: The product complies with the PGSSI-S user electronic identification repository. The product implements at least one electronic identification means within the framework of the transitional electronic identification means (with an enhanced 'eIDAS' guarantee level) as defined by the above-mentioned reference framework. Where appropriate, the product uses one or more means of electronic identification among: eIDAS-certified electronic identification means of a substantial or high guarantee level; the motive map application Vitale.
- ✓ Level 3: The same as the previous level, other than: The product does not implement any electronic identification means within the framework of the transitional electronic identification means defined in the PGSSI-S user electronic identification repository.

04.05 - Rights management and separation

- Level not applicable: Always applicable if the criterion appears
- Level 0: No separation of rights is implemented in the product.
- Level 1: A separation of rights is ensured in the product. In particular, product technical administration permissions are distinct from business authorisations (i.e. a technical administrator does not automatically have access to business functions and information)
- ✓ Level 2: The same as the previous level, plus: Permissions can be managed by profiles, and users by groups.
- ✓ Level 3: The same as the previous level, plus: Authorisations controlling the management of authorisations and those controlling the management of traces are all separate authorisations from all others. A separation between potentially incompatible authorisations (e.g.: 'applicant' and 'validator') is in place for business processes that justify it, or it has been verified that there are no such potentially incompatible authorisations.

❗04.08 - Use and updating of national identities of natural health stakeholders

- Level not applicable: Always applicable if the criterion appears
- Level 0: The product does not have the ability to identify legal health stakeholders using a national identity (legal FINESS, geographical FINESS, SIREN or SIRET).
- Level 2: The product identifies the legal health stakeholders using a national identity in accordance with the PGSSI-S electronic identification repository of legal health stakeholders. These identities are editable through a documented management process.
- ✓ Level 3: The same as the previous level, plus: The documented management process systematises searches/verifications with the Reference Directory and limits changes to attributes that are absent from the national identity as visible on the Health Directory and other exposure layers of the FINESS and SIREN repositories. Checks on these exposure layers are carried out on a regular basis or in connection with transactions carried out by the users concerned (electronic identification, etc.), in compliance with applicable regulatory requirements.

❗04.09 - Guarantee level of electronic identification of natural health stakeholders

- Level not applicable: Always applicable if the criterion appears
- Level 0: The product does not implement electronic identification of its legal health stakeholder users.
- Level 1: The product ensures the electronic identification of its legal health stakeholder users, but it does not allow the user structure to comply with the requirements of the PGSSI-S legal health stakeholder electronic identification repository.
- ✓ Level 2: The product ensures the electronic identification of its legal health stakeholder users, and allows the user structure to comply with the requirements of the PGSSI-S electronic identification repository for legal health stakeholders. In particular, if the product is likely to be implemented within the context of shared digital services, it allows the authentication of legal health stakeholders via certificates issued by IGC Santé. Where the product includes an SaaS service, it shall be implemented in accordance with the PGSSI-S electronic identification repository of legal health stakeholders, in particular as regards the type of electronic identification means used.
- ✓ Level 3: The same as the previous level, plus: In the event that the product includes an SaaS service that is part of shared digital services, the electronic identification is exclusively based on legal person authentication certificates issued by IGC Santé.

07. Auditing

❗ 07.02 – search for vulnerabilities

- Level not applicable: Always applicable if the criterion appears
- Level 0: No intrusion tests or vulnerability tests were performed on the product.
- Level 1: Vulnerability scanners check all components of the product before making available a new version. Vulnerabilities identified by vulnerability scanners or during an intrusion test result in an action plan for correction thereof.
- ✓ Level 2: The same as the previous level, plus: An intrusion test is also carried out on the product at least annually. The presence of a major vulnerability, identified by a scanner or intrusion test, blocks the availability of the new version and triggers a new development cycle at the end of correction. The list of residual vulnerabilities and their impacts is made available to the user structures' RSSIs. In case of detection of a major vulnerability on an existing version of the product, the user structures' RSSIs shall be immediately alerted and palliative measures applied until a patch is communicated to them as soon as possible.
- ✓ Level 3: The same as the previous level, plus: An intrusion test is also carried out on the product before any new version with major changes is made available.

08. Maintaining a secure state

❗ 08.02 - Monitoring and patch management

- Level not applicable: Always applicable if the criterion appears

- Level 0: Neither monitoring nor a patch management process is defined and implemented with respect to the components of the product supplied to the manufacturer by third parties, the platforms with which the product is deemed compatible, or generic vulnerabilities that may affect the product.
- ✓ Level 1: A process of monitoring the vulnerabilities of the product components provided to the manufacturer by third parties, and applying patches or updates to those components is defined and applied. In the case of software or platform-type products, such updates shall give rise to the availability of a new version of the product, and the user structure shall be notified thereof. In the event of a serious vulnerability, the user structure shall be notified as soon as possible and palliative measures shall be communicated to it as soon as possible, pending a product update.
- ✓ Level 2: The same as the previous level, plus: if the product requires, for its operation, a particular technical environment which is not part of its components (e.g. an operating system, a data base management system, etc.), a process for monitoring updates to this environment is defined and applied. The product is tested with any standard update of this environment. In the case of software or platform-type products, in the event of malfunction of the product linked to an update of that environment, the user structure shall be informed of this and the palliative measures shall be communicated to it if they exist. A new version of the product compatible with the update of the environment is made available as soon as possible.
- ✓ Level 3: The same as the previous level, plus: A patch management industrialisation process is implemented. It makes it possible to patch and test the product in order to ensure its proper functioning with all the evolutions applied. In the case of software or platform products, the product requires for its operation a particular technical environment, a dashboard accessible to the user structure allows it to consult the explicit compatibility of the product with the different patches or versions of the operating environment of the product.

❗ 08.03 - Obsolescence management

- Level not applicable: Always applicable if the criterion appears
- Level 0: No obsolescence management process is defined and applied for the components of the product supplied to the manufacturer by third parties and the platforms with which the product is deemed compatible (in the case of software or platform/applicable products) or on which the product is actually operated (in the case of service-type products).
- ✓ Level 1: Components supplied to the manufacturer by third parties are replaced in the product when they have reached the end of their support lifetime by their publisher/manufacturer. The product is adapted to a version of its environment (e.g. operating system, data base, etc.) supported by its editor/manufacturer when the current version reaches the end of its support lifetime.
- ✓ Level 2: The same as the previous level, plus: The replacement of the components and the adaptation of the product to a supported version of its operating environment shall be carried out at least 6 months before the announced end of support for these elements. In the case of software or platform-type products, the user structure shall be informed within the same period of time of this development, as well as of the specific migration procedure associated with the product as appropriate.
- ✓ Level 3: The same as the previous level, plus: The replacement of the components and the adaptation of the product to a supported version of its operating environment shall be carried out at least 1 year before the announced end of support for these elements.

09. Business continuity

❗ 09.01 – Crisis management

- Level not applicable: Always applicable if the criterion appears
- Level 0: No crisis management procedures are in place.
- Level 1: A crisis management procedure is defined and known to the stakeholders concerned. However, no advisory note has been drawn up. The list of people to be mobilised or contacted in the event of a crisis, with their contact details, is not written or not kept up to date. The crisis situations considered are those that occur in the environment of the supplier of the product

(development/integration environment, operating environment for an SaaS product, etc.) or within the user structure (for a software product, appliance, etc.) when the product is impacted by the crisis situation, or seems to be one of the causes.

- ✓ Level 2: A crisis management procedure is defined and known to the stakeholders concerned. The list of people to be mobilised or contacted in the event of a crisis is drawn up and kept up to date with their contact details. Advisory notes (by type of scenario) are available in order to allow effective responses.
- ✓ Level 3: The same as the previous level, plus: Crisis management is regularly tested to assess and improve its effectiveness

09.02 - Business continuity plan

- Level not applicable: Always applicable if the criterion appears
- Level 0: No Business Continuity Plan (BCP) is in place.
- ✓ Level 1: The product managers know the conditions for launching the BCP and the different tasks to be carried out when the BCP is to be launched. However, there no written documents on this subject. The processes are known but are not all formalised in writing.
- ✓ Level 2: A business continuity plan exists and includes all the necessary information. However, this plan and all the documents constituting it are not regularly tested.
- ✓ Level 3: A business continuity plan exists and includes all the necessary information. It is reviewed periodically and in the event of a change in the product or organisation. The BCP is tested at least annually to assess its effectiveness.

09.04 – Output of safeguards

- Level not applicable: Always applicable if the criterion appears
- Level 0: No specific process of offline product backup is planned.
- ✓ Level 1: Procedures for offline backup and restoring product configuration and data are documented. In the case of hosted service or SaaS-type products, the backup procedure is actually implemented as documented. In addition, in the case of platform/appliance products integrating the backup solution, or hosted service or SaaS-type products, backups are made on media that are kept completely offline.
- ✓ Level 2: The same as the previous level, plus: Documented procedures include a proper backup verification procedure and also cover the software components of the product. A method is provided to calculate the storage space required for backups based on the intended use of the product and the desired period of retention. In the case of hosted service or SaaS-type products, the backup is done at least daily and the backup test and restoration procedures are carried out on a regular basis.
- ✓ Level 3: Conformant with the previous level, plus: the product is a hosted service or SaaS; or backup-related procedures and mechanisms are designed to enable backups/restoration to be carried out using versatile third-party backup tools while ensuring a consistent state of the backup, and do not compel the use of a specific backup product integrated or not integrated into the product.

11. Hosting

11.01 - Hosting of health data

- Level 0: The applicant or a third party under its responsibility hosting all or part of the components of the product, or providing all or part of the service in the form of a service (SaaS), has not obtained HDS certification.
- ✓ Level 1: The applicant or a third party under its responsibility, hosting all or part of the components of the product, or providing all or part of the service as a service (SaaS), has obtained HDS certification from a certifying body accredited by COFRAC (or equivalent at European level).

d. Quality of content

QUA Quality of content

- QUA.1.1B Respondents' expertise

  The medical/health content of the digital service MUST be selected, validated and/or drafted by a committee whose collective expertise covers the subject matter of the digital service. The names, qualifications and links of interests of these persons MUST be made available to users and easily accessible.

  - Supporting documents: Names, qualifications and links of interests of the experts implicated in the selection, validation and/or drafting of the medical/health content, proof of accessibility of the information (screenshots of the pages providing the information and the navigation indications allowing access to it).
  - Details of parts in Convergence
    - 1. List of respondents

      Evaluate or redirect to the list of experts who have selected, validated or written each piece of medical content with their name and qualifications. Distinguish between those who participated in the drafting of the medical content published in the service and the persons who validated this medical content.
    - 2. Declaration of conflicts of interest

      Indicate (or redirect to) the experts' declaration of conflicts of interest
    - 3. Accessibility of information

      Provide the pages/places that can be accessed online that provide the information in 1. and 2. (screenshots with access paths, links to website URLs, etc.), if possible distinguishing between those produced and those taken over from an external organisation.

- QUA.1.2B Scientific references

  The medical content of the digital service MUST comply with the recommendations of organisations whose information is deemed reliable. If developed from scientific references, these shall be searchable. All sources used for the drafting of medical/health content shall be easily accessible to users, for example on a dedicated page of the digital service or as references before or following the content.

  - Supporting documents: any document ~~capable of~~ attesting to the measures taken to ~~achieve the criterion~~ meet the criterion, in particular the list of scientific sources and references, as well as the screenshots of the pages providing the information and navigation indications allowing access to it.

  1. Details of parts in convergence
     - 1. List of sources and scientific references

     Indicate or redirect to – the list of organisations behind the content and the updated URLs of the associated websites (intra-App, resource website, external documentation, end-of-content reference, etc.~~...~~).
     Indicate the list of scientific references used.
     - 2. Information accessibility

     Provide the online searchable places that provide the information (screenshots, links to the URLs of the website, etc.).

- QUA.1.3 Monitoring process

  The digital service MUST include a monitoring process of scientific sources and references relevant to the development of medical/health content in order to reflect the current state of knowledge. This information shall be easily accessible to all. The user shall be informed of the date of updating of the content he or she consults.

1. Supporting documents: summary report of the monitoring and content updating of the strategy, as well as screenshots of the pages delivering the information and navigation directions to access such.
2. Details of parts in convergence
    - 1. Monitoring and updating of the strategy

    Describe the strategy for monitoring and updating key sources and scientific references (including frequency) and the main experts in charge of monitoring with their names and qualifications.
    - 2. Information accessibility

    Provide the places where the information update date is published and how the update is put forward to the user (screenshots, links to website URLs, browsing paths, readability of information, results of satisfaction surveys/user groups, etc.). In case of transmission of the results of a user survey, specify which question assesses the ease of access of information concerning the monitoring process.

- QUA.1.4 Clinical evaluation and evidence Information documenting the performance, clinical or organisational interest of the application, as well as opinions issued within the context of claims for reimbursement by national solidarity MUST be easily accessible to users. Failing this, information relating to the absence of data documenting the clinical or organisational interest shall be made available to users of the digital service. This information and the evidence shall be easily accessible to users.
    1. Supporting documents: any document ~~that can~~ attesting to the measures taken to meet ~~achieve~~ the criterion, including any document describing the clinical evaluation of the service and justifying the accessibility of the information. In the absence of a clinical evaluation, any documents proving the accessibility of this information.
    2. Details of parts in convergence
        - 1. Evaluation of the service

        Where it exists, describe the clinical evaluation carried out (description of the design of the clinical study, the results obtained and their level of evidence)
        - 2. Information accessibility

        Provide evidence of the accessibility of the information made available to users (screenshots, links to the URLs of the website, etc.~~...~~). This information may be:
            - ~~p~~Publications in peer-reviewed scientific journals, protocols, study reports~~;~~
            - P~~p~~ublic information from test data bases on ongoing, upcoming or unpublished studies~~;~~
            - A~~a~~ statement indicating the lack of available clinical data to document the interest, be it clinical or organisational~~;~~.
            - ~~t~~The opinion or opinions of the CNEDiMTS in the event that the solution has been assessed within the context of a request for reimbursement by national solidarity (the most recent if it corresponds to the set of indications for which reimbursement has been claimed or the set of most recent notices corresponding to each of the indications for which reimbursement has been claimed).

- QUA.1.5 Interpretation by healthcare professionals

The interpretation of individualised health data, produced or transmitted by the user, MUST be carried out by professionals whose expertise is adapted to the subject matter covered and in accordance with the regulations in force, in particular on the exercise of healthcare professions.

1. Supporting documents: a summary of the interpretation procedure detailing, in particular, the list of persons qualified for this interpretation, their qualifications, and the health content depending on their field of expertise.
2. Details of parts in convergence
    - 1. List of health professionals qualified for interpretation

Describe who the health professionals are (with their names and qualifications) by recalling all health content and assigning to each health content at least one person qualified to interpret it.

- 2. Interpretation process

Describe when (first line, second line etc.) and how the interpretation is implemented.

- ℹ QUA.1.6 Implication of users (as this criterion ~~being~~ is optional, no assessment will be made in the initial assessment)

  Medical/health content of the digital service MUST be developed with the involvement of users representative of the target population.

  1. Supporting documents: any document ~~capable of~~ attesting to the measures implemented to meet ~~achieve~~ the criterion, and in particular all documents relating to the strategy of soliciting users in the development of the content of the digital service.
  2. Details of parts in convergence
     - 1. Describe the strategy for soliciting users in the development of the content of the digital service (analysis grid, Living Lab, etc.), number of users and/or list of user organisations implicated.

e. Ethics

ACC Accessibility – Terms of access to the service

- ❗ ACC.1.1 intuitivity and inclusion of all audiences

  The system MUST be developed with the intention of being intuitive, so that it is accessible to everyone and does not exclude any audience (cultural diversity, disability, literacy, etc.).

  1. Supporting documents:
     - ~~a~~Any document capable of attesting to the implementation of a method for assessing intuitivity
     - ~~a~~Any document attesting to the implementation of an accessibility assessment method
  2. Details of parts in convergence
     - 1. For example, transmit the RG2A certificate, multilingual documents.
     - 2. Indicate work in process to increase the accessibility and intuitiveness of the service. For example, specify whether the service exists in several languages, in particular Creole.
     - 3. If user tests have been carried out Describe the methodology – especially the users implicated by insisting on the diversity of the group (in terms of, for example, age, gender, disability, literacy level, SSC, etc.) - and the results of the tests. Example of tests: user groups, surveys, satisfaction surveys, etc.
     - 4. If there were no user tests Describe the format or method used to assess the service's ability not to exclude any audience and be intuitive (analysis grid, writing, living lab, etc.).

- ❗ ACC.1.3 Human support

  The system MUST provide a help and support service involving human interaction to help the user use the digital solution

  1. Supporting documents: any document that can attest to the measures taken to ~~achieve the criterion~~ meet the criterion, in particular a description of the help

service, a document attesting to the accessibility of the information on its existence, a description of the navigation path permitting access.

2. Details of parts in convergence
    - 1. Help and support service documentation
      Provide the documentation of the help and support service involving human interaction (including in particular ways of helping such as e-mails including the response time, telephone numbers with operating hours, etc.).
    - 2. Accessibility of information
      Provide the places where this information is published, as well as the navigation path to reach it (screenshots, website URLs, etc.).

- ℹ ACC.1.4 Online help (this criterion is optional, no evaluation will be done for initial evaluation)
  The system can provide users with a system usage assistance service (contextual help, online help, user manual, tutorial, guide, e-learning, etc.) in order to develop their learning capabilities
  1. Supporting documents: any document attesting to ~~capable of attesting~~ the measures taken to meet ~~achieve~~ the criterion, in particular all guidance documents for online help (screenshots).
  2. Details of parts in convergence
     - 1. Describe the strategy in this area and the elements made available to the user to facilitate the use of the service (contextual help, online help, user manual, tutorial, guide, e-learning, etc.).

- ℹ ACC.1.6 Critical decision alerts (~~this criterion being optional, no evaluation will be done for the initial assessment~~ as this criterion is optional, no evaluation will be done in the initial assessment)
  If a critical decision is produced by the system THEN the system must report an alert directly to the healthcare professional or to 15 to avoid any risk of misunderstanding by the user.
  1. Supporting documents: any document ~~capable of~~ attesting to the measures taken to ~~achieve the criterion~~ meet the criterion, in particular the risk analysis, the alert system and any prerequisites.
  2. Details of parts in convergence
     - 1. Provide a risk analysis according to the level of severity of the consequences in case of poor interpretation of the target information by the application.
     - 2. Describe the alert system in place and the calibration of its trigger. If there are prerequisites for the alert system to work, specify them (known phone number of the user, known email address of the user, etc.).

- ℹ ACC.1.7 Responses to questions (~~this criterion being optional, no evaluation will be done for the initial assessment~~ as this criterion is optional, no evaluation will be done in the initial assessment)
  The system documents, updates and makes accessible to users answers to frequently asked questions
  1. Supporting documents: any document ~~that can~~ attesting to the measures taken to ~~achieve the criterion~~ meet the criterion, and in particular any document attesting to the accessibility of the information, relating to frequently asked questions and the navigation route permitting access.
  2. Details of parts in convergence
     - 1. Provide the places where this information is published

- 2. Provide the navigation path to achieve this (screenshots, links to the URLs of the website, etc.).

ETH Ethics of transparency

- ℹ ETH.1.1 Understanding of the GDPR (this criterion being optional, no supporting documents will be required for the initial assessment)
  The system MUST ensure that the user understands the meaning of their consent within the context of the re-use of their personal data collected during the use of the application, in particular where there is commercial valuation of the data or apportionment of data with other stakeholders or subcontractors. The proper understanding of the user must also be ensured in the event of limitations to the GDPR rights, for example, the limitation of the rights to erasure of their data or portability.
  1. Supporting documents: any document ~~capable of~~ attesting to the measures implemented to achieve the standard, and in particular the method implemented to assess the user's understanding of the scope of their consent to the re-use of their data, the possible commercial valuation of their data, their possible apportionment with other stakeholders and the limitation of their GDPR rights.
  2. Details of parts in convergence
     - 1. Describe the means used to assess the user's proper understanding of the scope of their consent to the re-use of their data, their possible sharing with other stakeholders and the limitation of their GDPR rights as well as the results obtained (e.g. working groups, user surveys, etc.)
     - 2. If user tests have been carried out, describe the methodology – especially the users implicated by insisting on the diversity of the group (in terms of, for example, age, gender, disability, literacy level, SSC, etc.) - and test results (e.g. User groups, polls, user surveys, etc.)

- ❗ ETH.1.2 Consent

  For purposes for which the legal basis is consent, the system MUST implement mechanisms to allow 'à la carte' consent to the processing of data, allowing in particular to consent to the processing serving the main purpose(s) and not to consent to processing for secondary/accessory purposes.

  1. Supporting documents: Any evidence capable of proving that the user has the possibility of consenting to only part of the processing of their data.
  2. Details of parts in convergence
     - 1. Describe the 'à la carte' consent mechanisms: the service must offer separate consent for each of the purposes. Screenshot showing that there is no pre-ticked box. In case of transmission of the General Conditions of Use, please provide a screenshot of the location of the information concerned (page/paragraph).

- ❗ ETH.1.3 Identical service
  The system MUST offer an identical service regardless of the choices made by the user regarding the processing of their personal data
  - Supporting documents: any document ~~capable of~~ attesting to ~~the~~ measures taken to ~~achieve the criterion~~ meet the criterion, including a description of the means used to assess the identical nature of the service in different use scenarios and the results obtained.
  - Details of parts in convergence

- 1. Provide access to a demonstration account on the digital service, allowing to test usage scenarios regardless of the user's consent
- 2. If it is impossible to test these scenarios via the demonstration account, describe the means used to assess the identical nature of the solution in different use scenarios regardless of the user's consent:

o ETH.1.5 Configuration

The system MUST implement mechanisms so that users are able to configure the intensity of their interactions with the digital solution (e.g., configuration of notifications)

1. Supporting documents: description of the configuration of interactions
2. Details of parts in convergence
    - 1. Describe the mechanisms for modulating/setting the intensity of interactions with the digital solution (e.g. not receiving text messages in the evening and weekend) and the modalities of activation of these mechanisms by the user (e.g. a screenshot and the navigation path to obtain the explanations for configuration).

o ETH.1.6 Data erasure (this criterion being optional, no supporting documents will be required for the initial assessment)

The system implements mechanisms to allow the complete erasure of the data entered during the first stages of the use of the service if the user ultimately decides not to go through and to forgo the use of the service.

1. Supporting documents: Document describing the data erasure process.
2. Details of parts in convergence
    - 1. Describe the mechanisms for the complete erasure of data entered during the early stages of using the service if the user decides not to go through (e.g. data collected during the creation of an account) and waives the use of the service, as well as how users can implement them.

o ETH.1.9 Sensitive data(this criterion being optional, no evaluation will be done in the initial assessment)

If data likely to give rise to discrimination (such as religion, customs, orientation or sexual life of the person) are collected because they are necessary for the production of the service, THEN the system shall implement mechanisms to ensure that the user understands that the purpose of the collection is not discriminatory

1. Supporting documents: any document ~~capable of~~ attesting to the measures implemented to meet the criterion, including any document attesting to the accessibility of the information, and any document describing the method used to assess the understanding of the reasons justifying this collection.
2. Details of parts in convergence

    - 1. Accessibility of information
      Provide places where information on the reasons for collecting data that may give rise to discrimination is published.
    - 2. User comprehension
      Describe the means used to evaluate the user's good understanding of these reasons.

2. ETH.1.10 Benefits & Limits(~~this criterion being optional, no evaluation will be done for the initial assessment~~ as this criterion is optional, no evaluation will be done in the initial assessment)

The system implements mechanisms so that the user is able to understand the benefits and limitations of the service and chooses to use it in an informed manner

1. Supporting documents: any document ~~capable of~~ attesting to the measures implemented to meet the criterion, including any document attesting to the accessibility of the information, and any document describing the method used to assess the understanding of the benefits and limits
2. Details of parts in convergence

    - 1. Accessibility of information
      Provide locations where information on benefits and limitations of the service is published. NB: The benefits (advantages) are often listed in the GCU of the solution, on its home page, in a commercial brochure... Limits (disadvantages) often appear in the GCU, FAQs, or contextual pop-ups during use. For example, limits can include a low ecoscore result, partial performance, or functionality not covered by the solution. They generally indicate that the solution does not replace an emergency service and that in case of doubt the user should contact the SAMU or consult a healthcare professional.
    - 2. Understanding by the user
      Describe the means used to assess the user's good understanding of these benefits and limitations so that they make an informed choice.

INT Artificial Intelligence and ethics

An artificial intelligence system (AI) is a software, developed using one or more of the techniques and approaches listed below, capable of calculating results from input elements representing predictions, recommendations or proposals for decisions that may influence physical or virtual environments with which the SIA interacts. The different AI systems vary according to their level of autonomy and adaptability after deployment.

The techniques and approaches considered for this list of questions are as follows:

- Machine learning (MLA) approaches still called machine learning, including supervised, unsupervised or reinforced learning, which can use a wide variety of techniques, including deep learning. Generative AI systems that use this type of approach rely on deep digital neural networks to generate their results. AAA allow SIAs to identify patterns, structures, or relationships in the data and then use them to produce a result.
- Logical and knowledge-based approaches, incorporating (symbolic) reasoning, knowledge bases, inference motors in particular, inductive (logical) programming and expert systems.
- Statistical approaches, Bayesian estimation, research and optimisation methods.

- INT.1.1 Interaction with AI
  If the service integrates algorithmic processing produced by an AI THEN the system MUST inform the user that they are interacting with an AI solution.
    - Supporting documents: Document attesting to the accessibility of information.
    - Details of parts in convergence
        1. 1. Provide the places where the user is informed that they are interacting with an AI solution (screenshots, links to the website, etc.)

- INT.1.2 Documentation bias
  If the service integrates algorithmic processing produced by an AI THEN system MUST document and make available to all the performance levels and algorithmic biases of the AI solution
    - Supporting documents: Document attesting to the accessibility of information.
    - Details of parts in convergence

1. 1. Provide the locations where the performance level and algorithmic biases of the AI solution are published (screenshots, links to the website, etc.).

- ℹ INT.1.4 Drift detection (~~this criterion being optional, no evaluation will be done for the initial assessment~~ as this criterion is optional, no evaluation will be done in the initial assessment)

  IF the service integrates algorithmic processing produced by an AI THEN the system shall implement mechanisms to detect whether the AI system has 'drifted' and requires re-evaluation

  1. Supporting documents: Document describing early drift detection mechanisms.
  2. Details of parts in convergence

     - 1. Describe the mechanisms to detect early whether the AI system has 'drifted' and requires re-evaluation.

- ℹ INT.1.5 Explicability (this criterion being optional, no evaluation will be done in the initial assessment)
  If the service integrates algorithmic processing produced by an AI THEN the system shall implements mechanism to explain the proposals of the AI system. In the case of black box systems, other explanatory measures (traceability, verificability, etc.) are put in place
  - Supporting documents: Document describing explicability.
  - Details of parts in convergence
    - 1. Describe the mechanisms to explain the proposals of the AI system or to put in place other explanatory measures.

- ℹ INT.1.6 Avoid bias (this criterion being optional, no assessment will be made in the initial assessment)
  If the service incorporates algorithmic processing produced by an AI THEN the system shall implement mechanisms to avoid creating or reinforcing discriminatory biases throughout the life cycle of the AI solution
  1. Supporting documents: Document describing the mechanisms to avoid discriminatory bias.
  2. Details of parts in convergence
     - 1. Describe the mechanisms to avoid creating or reinforcing discriminatory bias throughout the life cycle of the AI solution.

DEV Sustainable development

- ❗ DEV.1.1 Ecoscore
  The system MUST be assessed against the environmental impact of its use using the ecoscore method provided by the DNS and NSA
  1. Supporting documents: the value of the eco-score corresponding to the service and the GDSL code of the script used for the final measurement.
  2. Details of parts in convergence
     - 1. Provide the screenshot of the ecoscore website with your published result https://ecoscore-appli.esante.gouv.fr.

- ℹ DEV.1.2B Ecodesign (since this criterion is optional, no assessment will be made in initial assessment)

The system is developed in accordance with the ecodesign principles, implemented at each stage of its life cycle, in a more comprehensive approach to sustainable development

1. Supporting documents: any document capable of attesting to the implementation of the ecodesign principles
2. Details of parts in convergence
    - 1. E.g. pass on Ecodesign score using NumEcoDiag proposed by the MiNumEco (https://ecoresponsable.numerique.gouv.fr/publications/referentiel-general-ecoconception/numecodiag/)
    - 2. Indicate the rate of employees of the company who are sensitised/trained in eco-design, digital environmental impact life cycle assessments, etc.
    - 3. Provide any evidence to demonstrate the publisher's commitment to a sustainable development approach (ecolabel awarded by independent bodies, GreenIT policy, annual CSR report, etc.)

- ℹ DEV.1.4 Low speed and old equipment (this criterion being optional, no evaluation will be required for the initial assessment)

The system is accessible with a low speed and on equipment that does not need to be of the latest generation.

1. Supporting documents: any document capable of demonstrating that the service is accessible at a low speed and usable with old equipment
2. Details of parts in Convergence:
    - 1. Low speed:
        - Concerning a web application: screenshots of the application with a 3G browser
        - Concerning a mobile application: activation of 3G mode and recording of operation in a video
    - 2. Old equipment: The service must be able to function properly on any product/platform that is still supported by its manufacturer/publisher/supplier, i.e. until its end of life officially communicated by that manufacturer.
        - Provide the list of operating system versions supported by the publisher

- ℹ DEV.1.5 Reduce consumption of data centres (this criterion being optional, no assessment will be made for the initial assessment)

The system retains architectural choices for hosting the digital solution to reduce resource and energy consumption

1. Supporting documents: Document actions to reduce consumption.
2. Details of parts in convergence
    - 1. Provide any evidence to demonstrate actions taken to reduce resource and energy consumption related to hosting (e.g. low energy use measures such as recovery of waste heat, limitation of the use of water resources for cooling purposes, limitation of terminal renewal, reduction of storage spaces (source: Act REEN https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044327272).

4. Security for referencing involving data exchange

Rule 01

- ❗ R01 - Information Systems Security Policy (PSSI)

The manufacturer MUST develop, maintain and implement a network and information systems security policy (PSSI).

The PSSI MUST cover the application subject to referencing in My Health Area and all application-related environments (production and non-production).

- Supporting documents: the Information Systems Security Policy – PSSI

Rule 02

- R02 – Risk analysis

The manufacturer MUST carry out and keep up to date a risk analysis. The scope of the risk analysis MUST cover the application subject to referencing in My Health Area and the underlying production information system. As a result of the risk analysis, the manufacturer MUST identify the sensitive assets and associated risks, the identified security measures to be implemented and the residual risks.

- Supporting documents: Risk analysis including the risk treatment plan and residual risks (the risk treatment plan must be updated on the date of referencing on My Health Area).

Rule 03

- R03 - Security audits

The manufacturer MUST define and implement an audit programme that allows assessment over time of the level of security of the application subject to referencing in My Health Area and the underlying Production Environment against known threats and vulnerabilities.

The audit programme MUST include a minimum three-year audit (aligned with the accreditation process, see Rule R04), which must be carried out by a qualified Information Systems Security Audit Provider (PASSI). This audit MUST include:

The audit of the configuration of servers and network equipment included in the perimeter of the service. This audit is carried out by sampling and must include all types of equipment and servers present in the service's information system, including those implicated in the operation and administration of the service;

The intrusion test against external access to the service;

If the service benefits from internal developments, the source code audit of the security features implemented.

- Supporting documents:
    1. Audit programme (audit types, frequency, scope, etc.);
    2. Latest audit reports:
        - Application intrusion tests to verify the implementation of security functions;
        - Application production environment-related SI intrusion tests;
        - Administration SI intrusion tests;
        - Code audit of the application to verify the implementation of security functions;
        - Configuration audit to verify the implementation of security and hardening rules on equipment (servers, network & security equipment).
    3. If the audit reports contain major anomalies, it will be necessary to present:
        - The action plan associated with the audit;
        - Evidence to establish that the corrective measures have been implemented

Rule 04

- R04 – Internal security approval

The manufacturer MUST carry out the internal security approval of the application subject to referencing in My Health Area.

- Supporting documents:
  1. Approval file.
  2. Approval decision (latest to date) bearing the signature of the internal approval authority of the manufacturer.

Rule 05

- R05 – Secure design and development of the application

The manufacturer MUST adhere to good safety practices when designing and developing the application subject to referencing in My Health Area.

The manufacturer MUST put in place appropriate security measures in the production environment but also on the user terminal side.

- Supporting documents:
  1. Audit report:
     - Application intrusion tests to verify the implementation of security functions.

Rule 06

- R06 – Secure configuration of information systems related to the application

The manufacturer MUST adhere to good secure configuration practices when installing services and equipment on the application's information systems subject to referencing in My Health Area.

The configuration rules aim at strengthening the level of security of the SI by hardening and include:

- The limitation and appropriate configuration of the functions present on the SI;
- The control of the material elements of the SI;
- The control and security of data integration vectors to the SI (such as removable media).

- Supporting documents:
  - Audit report:
  - Audit reports:
    - Application production environment-related SI intrusion tests.
    - Configuration audit to verify the implementation of security and hardening rules on equipment (servers, network & security equipment).
  - Description of the hardening measures used.
    - For the 'control of data integration vectors', the description of the antivirus policy (technical scope on which antivirus coverage is applied/not applied; procedure for monitoring antiviral alerts).
    - Latest configuration audit report to verify the implementation of security and hardening rules on equipment (servers, network & security equipment).
    - Latest application production environment-related SI intrusion test report.

Rule 07

- R07 – Cryptography

The integrity and confidentiality of the sensitive data of the application subject to referencing in My Health Area and the underlying production MUST be guaranteed and controlled using cryptographic mechanisms in accordance with the General Security Reference Framework (RGS) and the latest recommendations of the ANSSI in force.

- Supporting documents:
  - Description of protocols and algorithms for the protection of data integrity and confidentiality at rest and during transmission (these elements may appear during risk analyses).

Rule 08

- R08 – Partitioning and filtering

The manufacturer MUST carry out the partitioning of its information systems in order to limit the spread of security incidents within its systems or subsystems.

The manufacturer MUST put in place mechanisms for filtering data flows circulating in its information systems in order to allow only the data flows necessary for the operation and security of SI.

The manufacturer MUST implement a regular review of partitioning and filtering measures.

- Supporting documents:
  - Description of protocols and algorithms for the protection of integrity and confidentiality of data - Report of the review (internal or external control) of the application of partitioning and filtering measures.
  - Evidence that reviews of partitioning and filtering measurements are carried out regularly. This includes:
    - Formalisation of the frequency adopted by the manufacturer for the production of these reviews;
    - Record of previous reviews proving the completion of the reviews with the frequency defined by the manufacturer.

Rule 09

- R09 – Protection against remote access to the SI

The manufacturer MUST put in place security measures to protect the production information system from access via third-party information systems.

- Supporting documents:
  - Description of the architecture and mechanisms for protecting against remote access from workstations connecting to the SI associated with the application subject to referencing in My Health Area.

Rule 10

- R10 – Security of information systems administration

The manufacturer MUST create accounts (called ‘administrative accounts’) for the individuals (called ‘administrator’”) responsible for carrying out the administrative operations (installation, configuration,

management, maintenance, supervision, etc.) of the resources (infrastructure and applications) of the production SI underlying the application subject to referencing in My Health Area.

The hardware and software resources of the administration MUST be used exclusively to carry out administrative operations.

The manufacturer MUST conduct a regular review of administrative accounts.

- Supporting documents:
  - Description of the measures for the separation of privileges, the separation of the administrative SI and the resources used for the administration, accompanied by an architectural scheme of the administrative SI.
  - Report of the review of administrative accounts.
  - Reports of intrusion tests on the scope of the administration SI approved by the manufacturer.

Rule 11

- R11 – Identity and access management

The manufacturer MUST create individual accounts for all users and for all automatic processes accessing the resources of its information systems.

The manufacturer MUST protect access to the resources of the application and underlying information systems, whether by a user or by an automatic process, by means of an authentication mechanism involving a secret element.

The manufacturer MUST define, in accordance with its policy on security of networks and information systems, the rules for the management and allocation of access rights to the resources of the application and the underlying information systems.

The mechanisms of identification and authentication of users of the application MUST comply with the requirements of the Electronic User Identification Repository or the Electronic Health Stakeholder Identification Repository published by the Agency for Digital Health.

- Supporting documents:
  - Description of the rules of identification, authentication and access rights, formalised in an internal communication document (PSSI, password policy, identification procedure, authentication procedures, rights management procedure, account and access review report...).
  - Description of the architecture associated with electronic identification means.

Rule 12

- R12 – Maintaining a secure state

The manufacturer MUST develop, maintain and implement a process for maintaining a secure state for the hardware and software resources of the application subject to referencing in My Health Area.

- Supporting documents:

- Description of security maintenance processes.

Rule 13

- R13 – Event logging, correlation, analysis and detection systems

The manufacturer MUST implement organisational and technical measures for the logging, detection, correlation and analysis of security events of the application subject to referencing in My Health Area and the underlying production SI.

- Supporting documents:
  - Description of the logging system.
  - Description of the log correlation and analysis system.
  - Description of security incident detection processes.

Rule 14

- R14 – Response to security incidents and crisis management

The manufacturer MUST put in place a specific process to deal with security incidents and a crisis management process in the event of security incidents that have a major impact on the application and/or underlying SI, in accordance with the agreement for referencing in My Health Area.

The process MUST include a directory or procedure including a directory of correspondents to alert in case of crisis.

- Supporting documents:
  - Incident response procedure.
  - Crisis management procedure.

Rule 15

- R15 – Certification of Health Data Hosts

Hosts of applications subject to Article L. 1111-8 of the Public Health Code MUST be certified Health Data Hosts (HDS).

A justification must be provided where HDS certification is not applicable to the manufacturer.

- Supporting documents:
  - Up-to-date HDS certification covering the production SI underlying the application subject to referencing in My Health Area or a justification of the non-applicability.

5. Purposes

- **This box must be ticked by the publisher in order to continue to be referenced**

‘The digital tool or service may only access (read and/or write) the data of My Health Area, with the express consent of the holder, provided that such access pursues one of the following purposes: prevention, diagnosis, care, social and medico-social follow-up (Article L.1111-13-1 III of the Public Health Code). The data from My health Area to which the tool or digital service has access in this manner cannot be reused for any other purpose. ’